10 SCHRITTE FÜR MEHR CYBERSICHERHEIT

01 BACKUP

Sichern Sie regelmäßig Ihre Daten, archivieren Sie sie und sorgen Sie dafür, dass Sie jederzeit darauf zurückgreifen können. Lagern Sie die Datenträger mit den Sicherungen räumlich getrennt voneinander - außer Haus, anderer Brandschutzabschnitt.

02 VIRENSCHUTZ (SCHUTZPROGRAMME)

Der Schutz vor Malware ist eine der Hauptaufgaben eines Antivirusprogramms. Seien es Viren, Trojaner oder Ransomware - ein zuverlässiger Antivirenschutz ist gegen Bedrohungen aus dem Internet unverzichtbar!

03 IT-SYSTEME UND SOFTWARE AKTUELL HALTEN

Halten Sie Ihre IT-Systeme, mobilen Geräte und Dienste stets aktuell und überprüfen Sie diese regelmäßig.

04 SCHULUNG MITARBEITER:INNEN – SICHERHEITSBEWUSSTSEIN

Schulen und sensibilisieren Sie Ihre Belegschaft regelmäßig für das Thema IT-Sicherheit.
Verwenden Sie für die Schulung Ihres Personals das speziell entwickelte *IT-Sicherheitshandbuch für Mitarbeiterinnen und Mitarbeiter der WKO.*

05 NUTZUNG IT KLAR GEREGELT - PRIVAT / GESCHÄFT

In welchem Umfang dürfen Mitarbeitende das Firmennetz oder ihren Firmenlaptop privat nutzen? Eine schriftliche Vereinbarung dazu ist für jedes Unternehmen ratsam. Dies kann über den Arbeitsvertrag, eine Dienstvereinbarung oder extra Nutzungsregelung erfolgen. Beachten Sie dabei, dass diese Vereinbarung sowohl den zeitlichen als auch inhaltlichen Umfang der Nutzung festschreibt.
Achtung: Ist in Ihrer Firma beispielsweise das private Surfen im Netz auf Arbeitgeber-Rechnern üblich oder geduldet, kann das als stillschweigende Einwilligung Ihrerseits gelten.

06 PASSWORTRICHTLINIEN / 2FA

Achten Sie auf sichere Passwörter und setzen Sie nach Möglichkeit überall eine Zwei-Faktor-Authentifizierung ein. Die Zwei-Faktor-Authentifizierung ist eine zusätzliche Sicherheitsmaßnahme zum Schutz von Benutzerkonten. Neben dem Kennwort muss beim Login eine weitere Sicherheitskomponente bereitgestellt werden. Neben Fingerabdruck oder Smartcard kommt auch eine Verifizierung durch das eigene Smartphone (wie beim Onlinebanking) in Frage.

07 BENUTZER/USER-RECHTE - KEINE ADMIN-RECHTE / SOZIALE NETZWERKE

Erstellen Sie ein eindeutiges Berechtigungskonzept für Ihre IT-Systeme, in dem genau geregelt ist, wer welche Zugriffsbefugnisse hat. Stellen Sie für Ihre Belegschaft Richtlinien im Umgang mit sozialen Netzwerken auf, insbesondere welche Daten dort veröffentlicht werden dürfen.

08 RICHTLINIEN & GEBÄUDESICHERHEIT

Erstellen Sie gut verständliche Sicherheitsrichtlinien für Ihre IT-Systeme und legen Sie fest, welche Apps und Daten auf mobile Geräte übernommen werden dürfen. Stellen Sie auch die physische Sicherheit in Ihrem Gebäude sicher.

09 NEXT GENERATION FIREWALL

In Zeiten komplexer Cyberangriffe stoßen klassische Firewalls an ihre Grenzen. Aus diesem Grund bewerten Next Generation Firewalls z.B. EDR (Endpoint Detection & Response) den Datenverkehr nicht nur anhand von Ports und Protokollen - sondern anhand seines konkreten Inhalts.

10 NOTFALLPLAN & IT-DOKUMENTATION

Der Notfallplan ist das zentrale Dokument, um auf Notfälle in der IT angemessen und zügig zu reagieren. Ein Notfallplan und die IT-Dokumentation sind dabei die Leitfäden, um im Ernstfall so schnell wie möglich die IT wieder betriebsfähig zu machen, sowie das Schadensausmaß zu begrenzen.